



02-02-00

A

MICHAEL R. GILMAN\*  
JEFFREY I. KAPLAN

# KAPLAN & GILMAN, L.L.P.

COUNSELORS AT LAW

OF COUNSEL  
RONALD B. GOLDSTEIN  
FRANCINE M. MEYER

900 ROUTE 9 NORTH  
WOODBIDGE, NEW JERSEY 07095  
TELEPHONE (732) 634-7634  
FACSIMILE (732) 634-6887

73 CROTON AVENUE  
OSSINING, NEW YORK 10562  
TELEPHONE (914) 923-6240  
FACSIMILE (914) 923-6258

\* ADMITTED ONLY IN NY & CT

Date: February 1, 2000

Re: Inventor(s): Robert Karch

Title: **RULE BASED SECURITY  
POLICY ENFORCEMENT**

Attorney Docket No.: 125/1



Box NEW APP. FEE  
Assistant Commissioner for Patents  
Washington, D.C. 20231

Sir:

Submitted herewith is the above-identified patent application. Also enclosed are:

- 1) 1 sheet of an informal drawing (Fig. 1);
- 2) A self-addressed, stamped return postcard; and
- 3) A check payable to the "Commissioner for Patents and Trademarks" in the amount of \$345.00.

Respectfully submitted,

KAPLAN & GILMAN, L.L.P.

*Jeffrey I. Kaplan*  
Jeffrey I. Kaplan  
Reg. No. 34,356

JIK/pa

Enclosures

P:\JKaplan\Telran Technologies\cvr new patent appl for rule based security policy enforcement.doc

## CERTIFICATE OF MAILING

Express Mail mailing label number: EL069665521US  
Date of Deposit: February 1, 2000

I hereby certify that this paper or fee is being deposited with the United States Postal Service *Express Mail Post Office to Addressee* service under 37 C.F.R. §1.10 on the date indicated above and is addressed to Box NEW APP Fee, Assistant Commissioner for Patents, Washington, D.C. 20231

Paula M. Halsey

(Typed or printed name of person mailing paper or fee)

*Paula M. Halsey*  
(Signature of person mailing paper or fee)

001020" 50526460

EL069665521US

## **RULE BASED SECURITY POLICY ENFORCEMENT**

### **TECHNICAL FIELD**

5           This invention relates to the enforcement of security policies with respect to data base access, and more specifically, to an improved rule based access control mechanism that is preferably used to enforce security policies such as dynamic and static separation of duties, confidentiality, compliance and privacy.

### **BACKGROUND OF THE INVENTION**

10           In data access systems, often records are being accessed, modified, deleted, and added by various personnel on a daily or even hourly basis. In large organizations there could be hundreds of people accessing various records and changing them from time to time. It is important however, that security policies be enforced. For example, due to the potential for fraud  
15   and embezzlement, it is important that two or more people be involved in the total implementation of certain processes. Such a separation of duties policy reduces the potential for fraud because it requires that multiple people would have to conspire with each other in order to implement a dishonest transaction. Consider a record in a database created which reflects the ordering of a particular item. The company will incur a cost for such item, and approval is required. A record  
20   would be created in the database reflecting the order.

          When payment is made, it is preferable that a different entity be responsible for signing the check and making payment. This precludes the ordering entity from ordering items that should not be ordered. Thus, in order to draft and sign the check for payment for the order, an additional entity should be involved. This additional entity means that for someone to order and  
25   pay for goods for a particular purchase, at least two parties would have to be involved in any potential fraud. This greatly decreases the possibility of such fraud occurring.

          An example of another kind of security policy is conflict of interest, specifically a 'Chinese Wall Policy'. This policy prevents an analyst who is consulting for company A from accessing potentially sensitive information on company B, a competitor of company A. Thus preventing the  
30   analyst from providing company A with confidential information about company B (or making

recommendations to company A based on this confidential information). Separation of duties is considered to be an integrity policy while conflict of interest would be a confidentiality policy. Other security policies such as compliance to legislative regulations, and privacy are also enforced through security policies.

5           One prior art solution to enforcement of the separation of duties policy is to include a rule within the data access software that tests for the occurrence of a first action by a particular entity each time a specified second action is attempted. Specifically, the software simply includes a rule that if entity A is the particular entity which wrote the order, then entity A cannot process the transaction required to pay the invoice. Thus, each time an invoice payment is requested, the  
10       software would check to determine if the entity processing the invoice is the same entity that placed the order. If so, the transaction would be disallowed. Such a technique enforces a separation of duties and thereby minimizes the possibility of the occurrence of fraud.

          The implementation of such an arrangement is less than perfect and is not without significant cost. First, the variety of rules regarding who can do what during specific times or with  
15       specific other conditions often leads to complex code which is difficult to modify and debug. For example, each time any action is requested, the software has to check every possible combination of prohibited transactions to determine if permitting the desired transaction would violate any rule.

          Additionally, the execution time is greatly slowed by the fact that a large number of lines  
20       of code must be executed each and every time through any data access. This is extremely wasteful since, for the most part, most of the rules are not even needed unless certain other conditions apply.

          An additional problem is that the separation of duties policy of prior systems is primitive in its user interface. There is little notification to users of the particular problems being encountered,  
25       and there is little flexibility in terms of changing the rules for different conditions.

          Another prior art solution attaches attributes or labels to the transaction items that represent the objects on which operations require compliance with the separation of duties policy. These attributes maintain the history of operations on the object and rules are written that utilized

the information contained in these attributes. The major drawback of this approach is that unless these attributes were designed into the system from the beginning, it can be prohibitively expensive to modify large legacy systems to contain and maintain the necessary attributes.

Both solutions suffer from the drawback that they only solve the separation of duties problem. Other solutions must be implemented to enforce other security policies.

### **SUMMARY OF THE INVENTION**

The foregoing and other problems of the prior art are and a technical advance is achieved in accordance with the present invention, which relates to a method and apparatus for enforcing security policies in a user flexible manner. Moreover, the system of the present invention does not require a large amount of excess code, nor does it make any requirements for special attributes to be attached to the protected transaction items (i.e. objects.) It can also be applied to enforcement of multiple types of security policies.

In accordance with the teaching of the present invention, an object oriented rules based system is utilized which provides for an administrator to add Transient Rule Generator (TRG) rules which upon certain conditions occurring, will automatically generate transient custom rules. These transient custom rules will prevent the occurrence of some event only during a pre-defined relevant time period. Thus, if a particular condition X occurs, the data access software is automatically altered to preclude condition Y. At the expiration of condition X, the rule precluding action Y is then removed from the data access code. The administrator may also enter customized rules directly.

In additional embodiments, the user or some other designated recipient is given messages regarding the particular reason for the denial, and may also be notified when the denial of a particular action takes effect, or terminates. Further, the security policies may be based upon the role of the user, as opposed to his or her particular identity.

### **BRIEF DESCRIPTION OF THE DRAWINGS**

Fig. 1 is a functional block diagram of the components of the present invention.

## **DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT**

The arrangement of Fig. 1 is intended to implement the teachings of the present invention which can be used to enforce security policies without the problems described above with respect to the prior art. The arrangement of Fig. 1 a site specific domain model 102 is used by an editor 103 to selectively create Transient Rule Generator (TRG) Rules and customized template rules that are appropriate for a given environment, based on a set of Template Rules 104. The site specific domain model provides information that is specific to any particular data access environment. This includes actual table and file names, schema names, user names, role names etc. The editor 103 places these rules into a permanent storage area 107 (104 and 107 may be the same storage location, but this is not required). These rules are designed to generate new rules that prohibit certain data transactions from taking place. The TRG rules are accessed and read for further customization, then integrated into the data access management software 111 at particular times as described hereafter. Custom rules are loaded directly into memory 108. A request from a user 109 to access data 113 that meets the appropriate condition, produces an event 105 that will cause a TRG rule to create a transient customized rule 106 from a Template Rule previously loaded from the permanent storage 104, if the conditions specified in the TRG Rule are met. Rules are accessed in memory 108 and applied by data access management software 111 to the user request. A file access or database manager 112 and a communication function 110 are also represented in Figure 1. The user communications may take place via an intranet, the Internet, or any other available communications channel.

In operation, hundreds of users may be accessing data 113 with the file access or database manager 112 via the data access management software 111. The arrangement of Fig. 1 provides for the data access management software 111 to fire rules depending upon certain conditions. The rules are all stored together in a rules file 107.

If a particular condition exists or action is taken which should prohibit a second action Y from being implemented, the data access management software 111 will simply have a rule precluding Y. The rules file 107 includes that rule and the rule is loaded into memory 108 and

implemented for firing at 111 if and when condition X arises. At the end of condition X (e.g. the invoice has been paid) the rule prohibiting action Y is eliminated from software 111 and marked for archive from permanent storage 107 to an audit log 114.

As an example, we consider the order and invoice situation described above with respect to the prior art. Specifically, when it is desirable to prohibit an individual from paying an invoice, a rule precluding that individual from signing off to pay that invoice is loaded into the data access management software 111 and will fire each time an update to that invoice is attempted. This rule would be generated at 106 immediately upon the purchase order being placed 105. Thus, if an individual placed the purchase order, that purchase order transaction would cause the rule to be generated and integrated into the data access management software 111. The rule would then preclude the payment of an invoice by a particular individual, namely he or she who signed off on the purchase order.

The rule is only loaded when the specified user logs on to the system and is only tested when the user performs some action. Upon the invoice being paid, the rule no longer needs to occupy processing power in software 111, and the rule is immediately eliminated. Unlike prior systems, the rule need not be fired and return a false each time the payment of an invoice is attempted. That is, if the user did not enter the order, no rule exists for this user so no rule need be tested.

In the conflict of interest example of a "Chinese Wall", an analyst consulting for a specific company must be prevented from accessing information about companies that are competitive with that company. A new analyst who is not consulting for any companies will have the ability to access information from any company in the database. The event of that analyst selecting information about any given company 105, will cause a transient rule to be generated 106, then loaded into memory 108 and saved to permanent storage 107. This rule will then be used by the data access management software 111 to prevent the analyst from accessing 112 any information about competitive companies stored in the database or file system 113. This rule will remain in effect until some pre-defined event occurs that indicates the analyst is no longer violating a conflict of interest when accessing information on a competitive company. This may be

on the condition that the analyst has not accessed information for his previous company for some time period. This time period being considered to be long enough that information accessed is out of date and no longer considered sensitive or having any significant value. The event may be that all the information accessed by the analyst has been made public. The event may be an override issued by an authorized individual. The event may be the removal of the previous company from the database or the conflict set. At the notification of this event, the rule will remove itself from consideration in the data access management software 111 and mark itself as inactive to be archived for audit purposes from permanent storage 107 to an audit log 114. Upon this occurring, the rule might notify the user 109 or some other designated recipient 115 (via message or e-mail or some other form of notification 110) of her/his change of status. The recipient may be a person or another computer process.

In accordance with the teachings of the invention therefore, conditions are precluded under certain circumstances not by testing for the existence of the circumstance to determine whether or not to allow the action. Rather, upon the circumstance occurring, a rule that unequivocally disallows the action is placed into the data access management software. Moreover, the rule is maintained in the data access management software only for the minimum amount of time required to enforce the security policy. More specifically, the rule is only loaded when the specified user logs on to the system. The rule only fires during the duration of the condition under which a particular action is to be precluded, and only for the specified user.

In an enhanced embodiment, the user is notified of the particular time frame or condition that has caused his or her attempted action to be precluded. Thus, a user may be notified that because he was the individual signing the invoice, he may not pay that invoice. In this manner, the user will know that he can pay other invoices or can pay for that invoice if someone else places the order. Or that he cannot access information about a company because it would be a conflict of interest.

An expansion of the invention relates not to individual users but to particular roles. Thus, for example, the security policy may relate to an accounting department individual when compared to an individual in the role of Human Resources personnel. In such a scenario, a rule

precluding a particular role from accomplishing any one or more actions may be implemented on the condition that a particular condition has been met. The security policy is thus not based upon the identity of the individual, but upon the role in which that individual works.

Often roles are used to implement static separation of duties. Specifically, a clerk role may be able to enter an order, but cannot approve any orders. This is handled by the current invention through the customization of template rules, which occurs in the editor 103. These rules are static and thus do not require any dynamic behavior.

Audit trails and records keeping are also contemplated by the invention. Specifically, each transient rule that is created is archived along with its lifetime and statistics of its use. For example, each time an attempt is made to accomplish a precluded action, a system may log such an event for later review by security personnel. The system would then have a record of how many times during an interval that action Y was precluded and was attempted.

If action Y is attempted too many times during the interval that it is precluded, additional security could preclude action Y altogether, even after the interval is over, unless and until overwritten with a supervisory function. Notifications may also be sent to the individual's manager, security personnel or some other computer process informing them of the situation. It is anticipated that certain race conditions may occur where the user attempts to violate the security policy before the rule can be generated. Insuring that the rule is generated and active before the first transaction is allowed to complete prevents this. In the event that the transaction fails, the rule would be made inactive. Since it is likely that the user will attempt to re-try the transaction if it fails, the rule need not be removed, but will be re-activated when the user re-submits the transaction. If the transaction has not been successfully completed at the time the user logs off the system, the rule will be removed at that time.

While the above describes the preferred embodiment of the invention, various modifications or additions will be apparent to those of skill in the art. Such additions and modifications are intended to be covered by the following claims.



**WHAT IS CLAIMED:**

1. A method of enforcing security policies in a data access system, said method comprising:  
defining a first action as a condition;  
5 determining that a second action should not take place if said condition occurs;  
storing a rule for use by said data access system, said rule precluding said second  
action; and  
upon occurrence of said condition, utilizing said rule in said data access system.
2. The method of claim 1 wherein said condition is effectuation of a first transaction by a  
10 user and said second action is the effectuation of a related transaction by the same user.
3. The method of claim 1 wherein said condition is effectuation of a first transaction by a first  
user in a particular role, and said second action is the effectuation of a second transaction by a  
second user in a second role, the roles being either the same or different.
4. The method of claim 3 wherein the role of the first user and that of the second user are  
15 different.
5. The method of claim 2 wherein the condition is effective temporarily and then is  
rescinded.
6. The method of claim 2 wherein a user attempting to effectuate said related transaction is  
informed of said condition and advised automatically that said second action is prohibited pending  
20 the relinquishment of the condition.
7. The method of claim 2 wherein said first action is the ordering of goods or services and  
said second action is the payment for such goods or services.
8. Apparatus for enforcing security policies to increase security of data access management  
software, said apparatus comprising:  
25 a file of rules, said rules only being applicable to prevent specified data transactions by a  
first user upon the effectuation of specified transactions to modify the data by said first user;  
software for recognizing that said first user has effected said transaction, and

means for reading said file, locating said rules to prevent said specified data transactions, and integrating said rules into said data access management software such that said specified database transactions are prohibited.

9. Apparatus of claim 8 wherein further comprising means for eliminating the rule from the data access management software at the conclusion of a predetermined time or upon a predetermined condition.

10. A method of enforcing confidentiality in the form of a wall comprising the steps of:  
storing at least one rule that prohibits a known party from accessing specified information in a database or file;

upon a first specified condition occurring, modifying data access software to include said rule that prohibits said known party from accessing said specified information in a database or file;

said first specified condition being indicative of said known party having knowledge of a particular set of information; and

upon a second specified condition occurring, removing said rule and storing said rule for future use, said specified second condition indicating that said knowledge is no longer sensitive.

11. The method of claim 10 wherein said rule is generated from a template rule.

12. The method of claim 11 wherein said known party is defined as any individual engaged in a predetermined role.

13. The method of claim 10 wherein said user is notified of the occurrence of said second condition.

14. The method of claim 13 wherein said notification is via email.

15. The method of claim 10 wherein said knowledge is no longer sensitive because it has been made public or because a predetermined time has passed.

16. The method of claim 1 wherein said rule is generated from a template rule.

17. The method of claim 10 wherein some other individual, not the user, is notified of the occurrence of said second condition.

18. The method of claim 16 wherein said notification is via e-mail.
19. The method of claim 2 wherein some other individual, not the user, is notified of the occurrence of said second condition.
20. The method of claim 18 wherein said notification is via e-mail.
- 5 21. The method of claim 6 wherein the notification is via e-mail.
22. The method of claim 2 wherein another individual, not the user, is notified when the user attempts the prohibited second action more than once.
23. The method of claim 10 wherein another individual, not the user, is notified when the user attempts the prohibited second action more than once.
- 10 24. The method of claim 21 wherein the notification is via e-mail.
25. The method of claim 22 wherein the notification is via e-mail.
26. The method of claim 21 wherein the other individual is the users manager or supervisor.
27. The method of claim 21 wherein the other individual is responsible for data security.
28. The method of claim 22 wherein the other individual is the users manager or supervisor.
- 15 29. The method of claim 22 wherein the other individual is responsible for data security.
30. The method of claim 9 wherein the eliminated rule is saved in an audit log.
31. The method of claim 10 wherein the eliminated rule is saved in an audit log.
32. The method of claim 1 wherein the rule is not loaded until the specified user logs on to the system.
- 20 33. The method of claim 1 wherein the rule is only tested for the specified user.
34. The method of claim 10 wherein the rule is not loaded until the specified user logs on to the system.
35. The method of claim 10 wherein the rule is only tested for the specified user.
36. The method of claim 3 wherein the rule is not loaded until a user in the specified role logs on to the system.
- 25 37. The method of claim 3 wherein the rule is only tested for a user in the specified role.
38. The method of claim 12 wherein the rule is not loaded until a user in the specified role logs on to the system.

39. The method of claim 12 wherein the rule is only tested for a user in the specified role.
40. The method of claim 1 wherein the security policy is separation of duties.
41. The method of claim 1 wherein the security policy is compliance to regulation.
42. The method of claim 1 wherein the security policy is privacy of data.
- 5 43. The method of claim 21 wherein the other individual is a computer process.
44. The method of claim 22 wherein the other individual is a computer process.

## **ABSTRACT**

A rules based system enforces security policies in a data access management system.

- 5 The rules based system provides rules that preclude certain activities, but those rules are only implemented and fired upon certain conditions occurring. This results in certain actions being precluded when specified conditions are true, without additional software required to check for the condition each time the action is requested.

Figure 1.  
 Creation and Implementation of  
 Rules for the Enforcement of Security Policies

